I claim:

1. A process for restricting unauthorized operations by a computer user, comprising:

using a security executable to create a list of authorized operations for said computer user;

attaching a hook function to all new processes;

employing the hook function whenever a new application is started to send a message to the security executable, said message including a process id and path of the new application.

receiving said message from the hook function at the security executable and correlating to said list to determine whether the new application is authorized or not;

answering the message by the security executable when the new application is authorized to indicate so;

stopping the new application when the new application is not authorized.

2. A software system for restricting unauthorized operations by a computer user, comprising:

a first program module for automatically attaching to all new processes and for querying an ID of each said new process;

a second program module in communication with said first program module, said second program module building a list of allowed applications, retrieving the ID of each new process from said first program module, and terminating each process not identified on said list of allowed applications.

3. The software system for restricting unauthorized operations by a computer user according to claim 2, wherein said first program module is executable in user mode.

4. The software system for restricting unauthorized operations by a computer user according to claim 2, wherein said first program module is attached to new processes by tying into the USER32.

5. The software system for restricting unauthorized operations by a computer user according to claim 4, wherein said first program module is a Windows hook procedure.

6. The software system for restricting unauthorized operations by a computer user according to claim 5, wherein said first program module communicates with said second program module by sending a message with the process ID and path of the process being examined.

7. The software system for restricting unauthorized operations by a computer user according to claim 6, wherein said second program module communicates with said first program module when said process is authorized by answering said message with an indication that said process is authorized.

8. The software system for restricting unauthorized operations by a computer user

according to claim 6, wherein said second program module automatically terminates said process when not authorized.

9. A process for restricting unauthorized operations by computer users in a network environment, comprising the steps of:

maintaining a list of authorized processes and IDs for each computer user;

monitoring all new processes that are started and determining an ID thereof;

determining whether the ID of each started process is on said list;

allowing said process to continue when its ID is on the list;

terminating said process when its ID is not on the list.